ABSTRACT

An efficient hashing technique uses $\dfrac{w^2 + w}{2}$ operations to hash a string "w"

words long rather than the w^2 operations of the prior art. This efficiency is achieved by

squaring the sum of the key and the string to be hashed rather than forming a product of

5   the key and the string to be hashed.

$$h(m) = \left((m + a)^2 \bmod{}_p\right)\bmod{}_{2^l}$$